



DEPARTMENT OF THE ARMY
OFFICE OF THE ADMINISTRATIVE ASSISTANT TO THE SECRETARY
OFFICE OF THE DEPUTY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS
DIRECTORATE OF NETWORK SECURITY SERVICES-PENTAGON
6607 ARMY PENTAGON
WASHINGTON, DC 20310-6607

SAAA-IT-NS

28 AUG 2002

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Connection Approval Procedures (CAP) for OAA IT&C Managed Networks

1. REFERENCES.

- a. AR 380-19, Information Systems Security, 27 Feb 98.
- b. Message, DISA, DTG 121713Z Dec 95, subject: Defense Information Systems Network Secret IP Router Network (SIPRNet) Interim Network Connection Requirements.
- c. DoD 5200.1-R, Information Security Program, 13 Dec 96.
- d. Department of Defense (DoD) Directive 5200.28, Security Requirements for Automated Information Systems (AIS), 21 Mar 88.
- e. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Nov 99.
- f. Defense Information Systems Network (DISN) Network Security Policy, Draft, 3 Dec 99.
- g. Instruction, Chairman of the Joint Chiefs of Staff (CJCSI) 6211.02A, Defense Information System Network and Connected Systems, 22 May 96.
- h. DoDD C-5200.5, Communications Security, 21 Apr 90.
- i. DoDI 4660.2, Communications Security, 31 Jun 92.

2. PURPOSE. To provide guidance, requirements, procedures, and instructions to customers/users of the Office of the Administrative Assistant (OAA) to the Secretary of the Army, Information Technology and Communications (IT&C) network services. In specific, to provide information relative to the connection of customer/end-user organization systems/networks to OAA ITC managed unclassified and classified automated information systems (AIS)/networks.

3. **APPLICABILITY.** The provisions of this memorandum are applicable to all organizations requesting connection to an OAA IT&C managed network. Networks managed by OAA IT&C are located throughout the National Capital Region, to include the Pentagon reservation and designated renovation "swing space" areas. These managed networks provide connectivity to external networks, such as the Internet, NIPRNet, and SIPRNet.

4. **REQUIREMENTS.**

a. **General**

(1) References 1a through 1i of this memorandum provide security requirements for DOD/Army information systems/networks. The OAA, IT&C has authority and responsibility for selected systems/networks in the Pentagon Community. The provisions of this memorandum implement the security requirements to support those referenced directive requirements.

(2) Organizations requesting connection of their automated information system (AIS) to any OAA IT&C managed network must comply with the provisions of this memorandum.

(3) Organizations with current connections to any OAA IT&C managed network must submit a Connection Approval Procedures (CAP) package or have a current approved package on file. An ODIT&C Form 5E is not required if the CAP package is simply documenting an existing connection.

b. **Specific**

(1) Organizations requiring connection to OAA IT&C managed networks (classified or unclassified) are required to submit a memorandum prepared on the requesting agencies'/organization's letterhead stationery and signed by the organization's Head (DAA or Designated Representative, if different).

(2) Address the memorandum to Office of the Deputy for Information Technology and Communications, Director of Network Security Services- Pentagon (NSS-P), ATTN: SAAA-IT-NS, 1777 N. Kent Street, (Room 1500), Arlington, VA 22209, requesting an Approval to Connect (ATC) (Encl 1). An INTERIM request for connection must be submitted if the system/network to be connected is operating under interim authority to operate (IATO) in as opposed to a final authorization to operate (ATO). The memorandum must reference this memorandum and include the following:

(a) Evidence of Risk Acceptance by the cognizant Designated Approving Authority (DAA)¹. Submit one of the following:

(b) The full accreditation memorandum/Approval to Operate (ATO), for the system to be connected, signed by the responsible DAA¹.

(c) The interim accreditation memorandum/Interim Approval to Operate (IATO) for the system to be connected, signed by the responsible DAA.

(3) Minimum requirements to obtain an IATC and/or ATC are listed in the OAA IT&C CAP Requirements Trace ability Matrix (Encl 1).

RESPONSIBILITIES:

a. OAA IT&C DAA:

(1) Provide security program management (including vulnerability assessment, network monitoring, security engineering support, etc.) and systems accreditation for Army OAA IT&C customers throughout the Pentagon, swing-space areas and National Capital Region.

(2) Facilitate the overall connection approval process for OAA IT&C customers.

(3) Assess CAP packages for compliance and providing feedback.

b. All organizations: (connecting to OAA IT&C managed networks-Pentagon backbones)

(1) Abide by the Connection Approval Procedures published by the OAA Deputy for IT&C or his/her Designated Representative.

(2) Notify the Pentagon Computer Incident Response Team (PENTCIRT) of any suspected or verified security incidents or violations at (703) 695-CIRT (2478).

(3) Notify NSS-P of any changes to the security posture of their connected system.

(4) Maintain the security posture of their system in accordance with the system's accreditation status. If a system is physically relocated, the system must be reaccredited within 90 days, in accordance with AR 380-19/DoD 5200.28 Para 4.9.7. The OAA IT&C CAP must be followed using the recertification and reaccreditation process.

¹ If the system has not yet been accredited or granted an IATO, contact the ODIT&C Accreditation Manager at 703-588-6499.

(5) Anticipate changes to the certification documentation should systems be relocated, and plan to expedite the reaccreditation process exercised by the system's security personnel.

(6) Ensure the connected system is reaccredited at least every three years. Connected systems must also be reaccredited anytime implementation of changes could adversely affect the systems security posture. A copy of the accreditation information must be provided to NSS-P to update your CAP package.

(7) Maintain configuration management of customer-owned equipment connected to the OAA IT&C managed network.

(8) Provide NSA approved communications security (COMSEC) devices to meet any COMSEC requirements that are not met by the OAA IT&C managed network.

(9) Actively work to correct and/or manage all deficiencies documented in the customer system's accreditation memorandum or IATO.

(10) Ensure that all users/customers of your connected systems/network understand that all traffic on OAA IT&C managed networks is subject to monitoring to detect intrusions and attempts at unauthorized access and that each customer must:

(a) Ensure their users are aware that the network is subject to monitoring. At a minimum, customers will notify their users by means of the DOD log-in notice and consent banner that use of the network is subject to monitoring. Such notification should state that system use constitutes consent to monitoring.

(b) Prevent backdoors to OAA IT&C networks, SIPRNet, and NIPRNet. All traffic to and from the Internet, SIPRNet, NIPRNet, or external organizations must pass through the Pentagon backbone.

1 Any technology the customer may employ which restricts or limits NSS-P's ability to detect intrusions and unauthorized access must be mitigated by installation of an OAA IT&C approved intrusion detection capability which integrates with the Pentagon's central intrusion detection system.

2 Customers should contact NSS-P for assistance before implementing a Virtual Private Network (VPN), or any other technology that restricts or limits the ability to detect intrusions. NSS-P will evaluate the customer's proposed intrusion detection system to ensure that: 1) the intrusion detection system is effective and thorough, and 2) the intrusion detection system integrates with OAA IT&C's intrusion detection system, allowing OAA IT&C to detect.

(11) Ensure that all customers/users of your connected systems/network understand that a compromise in the integrity of one user/customer makes the entire network vulnerable.

(a) A customer with computer vulnerabilities represents a risk to all customers on the backbone. The NSS-P will conduct vulnerability assessments of systems connected to OAA IT&C managed networks in order to test the adequacy of network security. A customer with identified vulnerabilities will be notified and must correct security deficiencies immediately or risk being disconnected if connected to the Pentagon backbone.

(b) If the customer has a firewall, the customer must, at least once each year, allow OAA IT&C security personnel temporary access through the firewall or access behind the firewall to conduct a vulnerability assessment, to include war dialing. All customers other than Army may conduct their own vulnerability assessment as long as the vulnerability assessment format has been coordinated with OAA IT&C NSS-P and results are provided to the OAA IT&C NSS-P Vulnerability Assessment Team for review.

(12) Notify OAA IT&C NSS-P of any network/computer configuration changes prior to their implementation so that appropriate security countermeasures can be implemented.

(13) Provide Network Points of Contact (primary and alternate) to OAA IT&C NSS-P. These points of contact will assist in the processing and the implementation of their respective CAP.

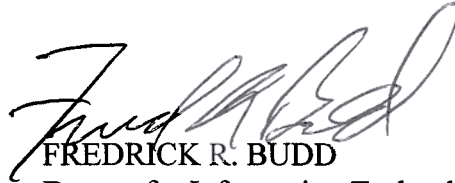
9. COMPLIANCE. Strict compliance with the provisions of the CAP is fundamental to the security of the network and the systems attached to the network and must be adhered to. If the customer/using organization fails to adhere to the CAP, and a clear risk to OAA IT&C managed networks/systems can be demonstrated, the customer/using organization will be given a maximum of 30 days to correct the compliance deficiency before the system is disconnected. In cases of severe and immediate risk, the system may be disconnected immediately.

10. EXCEPTIONS. Exceptions/exemptions/waivers will be considered on a case-by-case basis. Requests for waiver/exceptions/exemptions to any provision of these procedures must be submitted with full justification to the OAA IT&C Director of Network Security Services - Pentagon, ATTN: SAAA-IT-NS, 1777 N. Kent Street, Suite 1500, Arlington, VA 22209.

SAAA-IT-NS

SUBJECT: Connection Approval Procedures (CAP) for OAA IT&C Managed Networks

11. PROPONENCY. Proponent for these procedures is SAAA-IT-NS. The procedures will be reviewed/updated annually by the Director of Network Security Services-Pentagon.



FREDRICK R. BUDD
Deputy for Information Technology
and Communications

DISTRIBUTION:

Commander, AFPCA, Wash DC
Director, C3 Systems, EUCOM
Director, DIA
Director, IMCEN, ATTN: IASM
Director, MDA
Director, NIMA-Pentagon Operations Center
Director, OPT
Director, OSD CIO, ATTN: OSD DAA
Director, WHS, ATTN: DAA
HQDA, (DAAR-IM), Wash, DC
HQDA, (DAMI- IM), Wash, DC
HQDA, (DAMO-SPT-IMSO), Wash, DC
Chief, JSIRMO
Chief, NGB
ASBCA
ASG-IMD
DACH-IMR
DACS-GOM
DAIG
DAIM-MD
DAJA-IM-LTMO
DAMO-SPT-IA
DAPE-ZXI
DAPR-DPI

SAAA-IT-NS

SUBJECT: Connection Approval Procedures (CAP) for ODIT&C Managed Networks

DISTRIBUTION: continued

DTSW-OSS

JDHQSV-PAI

ODCS, G-4

PENREN/PM&SSG

SAAG-PMA

SAFM-LAN

SAIS-EIT

SAIS-ZXA-I

SAMR

SFAE-ISA-Z

SFMR-RBX-AS

SAAA-IT-AE

SAAA-IT-AR

SAAA-IT-BP

SAAA-IT-CM

SAAA-IT-DC

SAAA-IT-DT

SAAA-IT-IM

SAAA-IT-LS

SAAA-IT-NI

SAAA-IT-NS

SAAA-IT-PT

SAAA-IT-RM

SAAA-IT-TP

ENCL 1, OAA IT&C CAP Requirements Traceability Matrix, to OAA IT&C Connection Approval Procedures

The following constitute the minimum-security requirements for organizations that are accredited by the OAA IT&C DAA/Director of Security to obtain an IATC or an ATC to any OAA IT&C Managed network(s).

1. REQUIREMENT	IATC	ATC
Request for Connection Memorandum [As instructed in Paragraph 4 (b) See Sample letter in Encl 3] <i>Please include the following within the memorandum: 1) Mode of Operation (Dedicated/System High/ multi-Level etc) 2) Maximum Level of Sensitivity of Information being processed (Secret/Unclassified etc.)</i>	X	X
Statement of the current residual risk(s)	X	X
Consent to Monitor Statement	X	X
Pentagon Classified Backbone / SIPRNet Access Assessment Form (classified backbone connections) (SIPRNet Connections only)	X	X
Note: All other pertinent information will be extracted from the requesting organizations SSAA by the C&A/CAP personnel		

ENCL 1, OAA IT&C CAP Requirements Traceability Matrix, to OAA IT&C Connection Approval Procedures (continued)

The following constitute the minimum-security requirements for organizations not accredited by the OAA IT&C DAA/Director of Security to obtain an IATC or an ATC to any OAA IT&C Managed network(s).

2. REQUIREMENT	IATC	ATC
Request for Connection Memorandum [As instructed in Paragraph 4 (b)See Sample Letter in Encl 3] <i>Please include the following within the memorandum: 1) Mode of Operation (Dedicated/System High/ multi-Level etc) 2) Maximum Level of Sensitivity of Information being processed (Secret/Unclassified etc.)</i>	X	X
Full accreditation (ATO) memo signed by the cognizant DAA		X
Interim Approval to Operate (IATO) memo signed by the cognizant DAA	X	
Statement of the current residual risk(s)	X	X
Consent to Monitor Statement	X	X
System Architecture Connectivity diagram including IP addresses <i>(Diagram should only show gateway address between requesting organization and ODIT&C managed network)</i>	X	X
Approval for Open Storage (SIPRNet Connections only)	X	X
Pentagon Classified Backbone / SIPRNet Access Assessment Form (classified backbone connections) (SIPRNet Connections only)	X	X
Evidence of TEMPEST/EMSEC Survey (if applicable)	X	X
Information Assurance Security Officer (IASO) appointment memo		X
MOAs/MOUs (if applicable)		X
Joint Staff/OSD C3I Approval (Only for <u>all Non-DOD</u> connecting organizations)	X	X

ENCL 1, OAA IT&C CAP Requirements Traceability Matrix, to OAA IT&C Connection Approval Procedures (continued)

The following constitute the minimum-security requirements where classified data resides and/or SECRET LAN drops terminate in areas not approved for Open Storage.

3. REQUIREMENT	IATC	ATC
Implement policy and procedures IAW DoD 5200.1R to protect classified information during and after working hours	X	X
Ensure that protection/control mechanisms for access to secure drops are properly installed (e.g., Hoffman Box configurations)	X	X
Implement policy and procedures to control access to and protection of workstations	X	X
Ensure all workstations provide password-protected, timed screen savers	X	X
Ensure proper orientation of CRT away from points of ingress and egress	X	X
Ensure that DISA SIPRNet policy and DoD 5200.1R requirements are in-place to prevent unauthorized electronic access to PSB and SIPRNet	X	X
Establish policies and procedures to protect printer output IAW DoD 5200.1-R	X	X
Prevent infrared and wireless access by disabling the IR port and internal microphones on workstations.	X	X

ENCL 2, Request for Information Technology (IT) Products and Services, to OAA IT&C Connection Approval Procedures

**REQUEST FOR INFORMATION TECHNOLOGY (IT) PRODUCTS AND SERVICES
(ODIT&C Form 5-E)¹**

REQUEST FOR INFORMATION TECHNOLOGY (IT) PRODUCTS AND SERVICES		
<small>For use of this form, see ODIT&C Network Security Services—Pentagon New Requirements Team</small>		
1. ODIT&C TRACKING NUMBER	2. DATE RECEIVED	3. DATE NEEDED
4. REQUESTER (NAME/GRADE/ORG/OFFICE SYMBOL/PHONE)		5. CLASSIFIED PROCESSING <input type="checkbox"/> YES <input type="checkbox"/> NO
6. REQUIREMENT TITLE		
7. REQUIREMENT (Describe product or service required)		
APPROVAL AUTHORITY		
8. ACCOUNTING CLASSIFICATION	9. FINANCIAL ADVISOR SIGNATURE	
10. PRINTED NAME/GRADE/PHONE NUMBER OF IMO/URO	11. IMO/URO SIGNATURE	
12. ODIT&C APPROVAL AUTHORITY	13. ODIT&C APPROVAL AUTHORITY SIGNATURE	

ODIT&C FORM 5-E (Aug 00)

ODIT&C Form 5-E and Instructions for Completion of ODIT&C Form 5-E can be found on the Intranet (<https://secureweb.hqda.pentagon.mil/nisap/intra/>).

ENCL 2, Request for Information Technology (IT) Products and Services, to OAA IT&C Connection Approval Procedures (continued)

Instructions for Completion of ODI&C Form 5-E, Request for Information Technology Products and Services

BLOCK 1. ODI&C TRACKING NUMBER. The 6-digit number assigned by OAA IT&C Requirements Help Desk to identify each project in the requirements tracking database. The tracking number includes the last two numbers of the fiscal year, a dash, and the four digit sequential number of the requirement (e.g. tracking number 99-0900 indicates this is the 900th requirement received in fiscal year 1999).

BLOCK 2. DATE RECEIVED. Indicates the day OAA IT&C Requirements Help Desk received and logged a requirement.

BLOCK 3. DATE NEEDED. IMO/URO will coordinate with their customer to determine a realistic date when the required capability is needed (usually the required operational date [ROD]).

BLOCK 4. REQUESTER. Requesting official will state name, grade, organization, office symbol, and telephone number in this block.

BLOCK 5. CLASSIFIED PROCESSING. The requesting official shall indicate whether the desired IT product or service must process, receive, or transmit classified information.

BLOCK 6. REQUIREMENT TITLE. The requesting official must state the IT product or service capability desired.

BLOCK 7. REQUIREMENT. The requesting official should succinctly describe the IT product or service capability required. A description of what capability exists now may be helpful in determining the desired outcome state. The requesting official should describe why the capability is needed and the impact if the desired capability is not provided.

BLOCK 8. ACCOUNTING CLASSIFICATION. Financial Advisor provides the fund cite for the requirement in this block.

BLOCK 9. FINANCIAL ADVISOR SIGNATURE. Financial Advisor signs name in this block.

BLOCK 10. PRINTED NAME/GRADE/PHONE NUMBER OF IMO/URO. IMO/URO prints name, grade, and duty phone number in this block.

BLOCK 11. IMO/URO SIGNATURE. IMO/URO signs in this block.

BLOCK 12. ODI&C APPROVAL AUTHORITY. Appropriate OAA IT&C Approval Authority prints name, grade, and office symbol in this block.

BLOCK 13. ODI&C APPROVAL AUTHORITY SIGNATURE. Appropriate OAA IT&C Approval Authority signs in this block.

ENCL 3, Sample Request for IATC and/or ATC, to OAA IT&C Connection Approval Procedures

YOUR AGENCY LETTERHEAD

(Office symbol)

date

MEMORANDUM FOR Director, Network Security Services – Pentagon (NSS-P),
ATTN: SAAA-IT-NS, 1777 N. Kent Street (Room 1500), Arlington, VA 22209

SUBJECT: Request for Approval to Connect (ATC) to the Pentagon [Network Name]

1. Reference, memorandum, OAA IT&C NSS-P, SAAA-IT-NS, __ Aug 02, subject: Connection Approval Procedures (CAP) for OAA IT&C Managed Networks.
2. In accordance with the reference above, request that the (office/agency name) be granted an *[Interim]* Approval to Connect (ATC) the (network name), located at the Pentagon, Washington, DC. (or other location), to the (appropriate Pentagon backbone). The (office/agency system or Network Name) is authorized to operate in the *[System High, Dedicated, or Multi Level]* mode of operation with a maximum level of sensitivity for information being processed as *[Unclassified, Sensitive but Unclassified, Confidential, Secret, or Top Secret]*. A copy of the *[Approval to Operate/Interim Approval to Operate]* memorandum for the (network name) is attached as enclosure 1.
3. There *[are or there are not any]* known significant vulnerabilities on the (office/ agency system or Network Name). (Describe vulnerabilities and what is being done to mitigate them.)
4. The (office/agency system or Network Name) consists of equipment as shown on enclosure 2 (Hardware List). The (office/agency system or Network Name) *[is or is not]* connected to (the name of other network/networks using NSA-approved and tested high assurance guards). Customer local area networks are also connected to the (office/agency system or Network Name) as shown in enclosure 3 (topology diagram). The (office/agency system or Network Name) *[is or is not]* connected to contractor, foreign, non-DOD agency, or exercise facilities. Any Memorandums of Agreement (MOA) pertaining to the (network name) are attached as enclosure 4.]

ENCL 3, Sample Request for IATC or ATC, to OAA IT&C Connection Approval Procedures (continued)

5. A memorandum granting OAA IT&C consent to monitor the (office/agency system or Network Name) is attached as enclosure 5. Enclosure 6 is a Pentagon Secret Backbone/SIPRNet Access Assessment (SAA) Form. (*– only needed for connection to the Pentagon Secret Backbone.*)
6. This network [*is or is not*] accredited to send and receive NATO classified documents up to NATO Secret.
7. In addition, I formally agree to accept any and all risks associated with the establishment of the network connection between the OAA IT&C managed (network name, e.g., Pentagon Secret Backbone/Secret Internet Protocol Router Network (SIPRNet) Network) and the connecting system described above.
8. My point of contact for this action is (name of point of contact) (703) 999-9999.

Signature block of DAA or Agency Chief

Enclosures:

1. DAA's ATO/IATO Memorandum
2. Hardware List
3. Topology Diagram
4. MOAs (if any)
5. Consent to Monitor Memorandum
6. Pentagon Classified Backbone/SIPRNet Access Assessment (SAA) Form (if needed)

ENCL 4, Mode of Operations Descriptions, to OAA IT&C Connection Approval Procedures

MODE OF OPERATIONS DESCRIPTIONS

System High – A mode of operation wherein all users having access to the AIS possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval.

Dedicated – A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories.

Multi Level – A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the AIS.

ENCL 5, Requirements for Statement of Residual Risk, to OAA IT&C Connection Approval Procedures

Requirements for Statement of Residual Risk

- DAAs or Representative/Services/Agency's Site letterhead
- Signature date
- Statement of Significant or Residual Risk to the DAAs or Representative/Services/Agency's System at the Users Location
- Assessment of the risk to confidentiality, integrity, availability, and accountability
- Assessment of the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence
- Evaluation of operational procedures and safeguards with respect to their effectiveness and ability to offset risk at the DAAs or Representative/Services/Agency's Site
- Signature, full name, and title of Senior Site Official

Sample Statement of Residual Risk

DAAs or Representative/Services/Agency's
Address

Date

SUBJECT: Statement of Residual Risk for SIPRNet, CCSD:

1. The residual risk to the DAAs or Representative/Services/Agency's is (minimal or other). This assessment is based on evaluation of the known and presumed threats to the system, the vulnerabilities associated with the DAAs or Representative/Services/Agency's system, and all employed protective countermeasures.
2. The risk to system and data confidentiality, integrity, availability, and accountability is being maintained to an acceptable level. The vulnerabilities of the system with respect to the documented threat, ease of exploitation, potential rewards to the threat agent, and probability have been minimized by means of an aggressive Risk Management Program.
3. This Risk Management Program is based on a continual evaluation of the operational procedures and safeguards of the DAAs or Representative/Services/Agency's network to determine their effectiveness and ability to offset the defined risk at the DAAs or Representative/Services/Agency's site.

Signature

DAA or Representative/Services/Agency

ENCL 6, Sample Equipment List – Connectivity Description, to OAA IT&C Connection Approval Procedures

Equipment List – Connectivity Description

Software	Approximate Number of Users	Software Maintainer
Windows NT Server	3	123 Company
Windows NT Workstation	100	123 Company
4. WORD	100	XYZ Company
Calendar Creator	3	ABC Organization
Adobe Acrobat 3.0	100	
Delrina Formfiller	100	
Delrina JetForm Designer	100	
Office 97 Pro	100	
Word 6.0	100	
Winzip	100	
Norton Anti-Virus	100	
Internet Explorer 4.1	50	
Netscape Navigator 4.5	50	
Toolbox	50	

1. Hardware: (List all hardware with applicable IP addresses and who owns/maintains the hardware. May include attachment. The hardware list should contain amounts and types of all terminals, servers, hubs, routers, switches, etc.) See example, Attachment 1, Hardware List for XYZ System below.

[Insert hardware list here]

2. Connectivity:

a. Physical Connections: (List any physical connections the system has which lead to outside of the certification boundary (PINT, NIPRNET, SIPRNET, etc.). List the specific security countermeasures (HTTP-S, SSL, TLS, KIV-7, KG-94, etc.) that are in place to deny unauthorized access.)

ENCL 6, Sample Equipment List – Connectivity Description, to OAA IT&C Connection Approval Procedures

Connectivity	Boundary	Countermeasures Utilized
Exchange Mail Servers	NIPRNET via Pentagon Sensitive But Unclassified Backbone	-Login/Password by the mail server -Raptor Firewall
Remote Access Servers	Plain old Telephone System (POTS) via GTE	-Login/password by the RAS
Web Servers	SIPRNET via Agency Name Classified Backbone	-Non-DoD addresses blocked by Router
Web-based Oracle D-Base	NIPRNET via Agency Name UNCLASSIFIED Backbone	-Non-DoD addresses blocked by Router -Login/Password by the D-Base -Encrypted by SSL (FIPS 140-1 compliant)
ISDN connection	Plain old Telephone System (POTS) via GTE	Encrypted by KIV-7
Fractional T-1 with AF/XR on XYZ AFB	Plain old Telephone System (POTS) via GTE	

b. Logical Connections: (List any logical connections the system shares with other systems located outside of the accreditation boundary (Trust Relationships, etc.). List what specific security countermeasures (IP Blocking, etc.) are in place to deny unauthorized access from these connections.)

Connectivity	Organization - Domain Involved	Reason for Connectivity	Security Countermeasures
1-way Trust Relationship (Org1 to Org2)	Org1 – Org2	E-mail Sharing	Access Controlled at Router
2 Way Trust Relationship with Org2	Org1 – Org2	Sharing files on each other's domain	Security Countermeasures provided by NOS (NT 4.0).

3. Cabling – (What type of cabling (Fiber, 10BaseT) or wireless devices are being utilized? If the system utilizes different versions of cabling, please specify.)

ENCL 6, Sample Equipment List – Connectivity Description, to ODI&C Connection Approval Procedures

4. Network Protocols: (What network protocols are being utilized? - Ethernet, Token Ring, TCP/IP, AppleTalk, etc.)

5. Server Protocol/Services: What ports are utilized on your servers and what applications, protocols and/or services are associated with them? (Note: This is not an all-inclusive list of protocols/services. You must include any that are active.)

Active Ports	Associated Applications/Protocol/Service	Server
TCP ports 512 through 514	BSD UNIX R Commands (rsh, rlogin, and so forth)	Not installed
TCP/UDP port 53	Domain Name System (DNS)	DNS Server
TCP ports 20 and 21		Web Server
TCP port 79		
TCP port 443	HyperText Transfer Protocol - Secure (HTTP-S)	
TCP port 6667	Internet Relay Chat (IRC)	
TCP port 88	Kerberos	
TCP/UDP port 111	Network File System (NFS)	
UDP port 123	Network Time Protocol (NTP)	
UDP port 2049	NFS	
TCP port 110	Post Office Protocol (POP) 3	
TCP/UDP ports 161 and 162	Simple Network Management Protocol (SNMP)	

6. (U) Estimated Lifecycle: When is the hardware/software expected to be updated?)

Component	Years
Servers	
Workstation PCs	
Monitors	
Routers	
Hubs	
Switches	
CSUs/DSUs	

ENCL 7, Sample Consent to Monitoring Statement, to OAA IT&C Connection Approval Procedures

Sample Consent to Monitoring Statement

Letterhead Stationery

Date

MEMORANDUM FOR Director of Network Security Services - Pentagon, ATTN: SAAA-IT-NS,
1777 North Kent Street (Suite 1500), Arlington, VA 22209

SUBJECT: Consent to Monitor Connection to the (Network Name)

In accordance with the requirements of Chairman Joint Staff Instructions (CJCSI) 6211.02A, Defense Information System Network and Connected Systems, 22 May 1996, and the OAA IT&C Connection Approval Procedures (CAP) memorandum, I acknowledge that ODIT&C Directorate of Security and the Defense Information Systems Agency (DISA) will conduct periodic monitoring of the *[OAA IT&C managed Backbone (NIPRNet/SIPRNet)]* and connected customer systems. We acknowledge and consent to OAA IT&C conducting an initial vulnerability assessment and periodic unannounced vulnerability assessments on our connected host systems to determine the security features in place to protect against unauthorized access or attack.

Signature

Chief Network Official or DAA
(DAA or Representative/Service/Agency's signature block)

**ENCL 8, Pentagon Classified Backbone/SIPRNet Access Assessment, to OAA IT&C
Connection Approval Procedures**

Pentagon Classified Backbone/SIPRNet Access Assessment

Organization (Service/Agency Name): _____

Location _____

Date: _____

Plain Language Address (PLA)(Government Only): _____

POC and Phone number: _____

System or Network Name: _____

Premise Router IP Address: _____

Network IP Address Ranges _____

This form is to be submitted with the initial request for connection and exercises. Additionally, this form is to be re-accomplished when there is a change to the approved configuration, recertification, or a change that affects the answers on file.

Circle or Highlight responses below.

Foreign National Access

- #1 Yes No Foreign nationals, to include Integrated Officers (Foreign nationals in US positions), **have physical access to areas** where workstations **connect directly or indirectly** to the SIPRNet.
(Example: If other than US personnel have access (escorted or unescorted) to the SIPRNet workstation areas, a Yes response is required.)
- #2 Yes No Foreign nationals, to include Integrated Officers, are **users** on workstations on a network or subnet **connected directly or indirectly** to the SIPRNet.
(Example: If other than US personnel have user accounts on SIPRNet workstations, a Yes response is required.)
- #3 Yes No Foreign nationals, to include Integrated Officers, are **users** on workstations on a **separate network connected directly or indirectly** to SIPRNet.
(Example: A Non US network connected to a SIPRNet connection or using SIPRNet backbone as a transport layer to another Non US network, a Yes response is required.)

Contractor Access

- #4 Yes No Uncleared contractors **have physical access to areas** where workstations on the organization network or its subnets **connected directly or indirectly** to the SIPRNet.
(Example: Uncleared contractor personnel, either in support of a Government contract or maintenance support, to include cleaning people, have access to SIPRNet workstations, a Yes response is required)
- #5 Yes No Uncleared contractors are **users** on workstations **connected directly or indirectly** to the SIPRNet.
(Example: Any contractor (Prime or Sub), US or Non-US, having a user account on the SIPRNet, a Yes response is required. Explain if the contractor is located within an U.S. Government, non-U.S. Government or Contractor facility.)
- #6 Yes No Cleared contractors at a non-DoD facility are **users** on workstations **connected directly or indirectly** to the SIPRNet. Contract Number(s): _____
(Example: Any contractor (Prime or Sub) at a non-DoD facility (including Contractor facilities) on a separate network such as an Educational Facility, a Yes response is required.)

**ENCL 8, Pentagon Classified Backbone/SIPRNet Access Assessment, to OAA IT&C
Connection Approval Procedures**

#7 Yes No Reference question #6. Are there any uncleared personnel providing support under this contract.
(Example: Any contractor personnel (Prime or Sub) that are providing administrative, logistical or services in support of the contract identified in number 6, a Yes response is required.

Network Connectivity - Include the Secret and Below Interoperability (SABI) Ticket Number (if Applicable) :

#8 Yes No The Organizational network, to include subnet(s) and workstation(s), connects to a network operating at any level other than US Only Secret either **with or without a high assurance guard** in place. Note: KVM or A/B Switchboxes are considered inter-network "connections".

(Example: A network operating at Unclassified But Sensitive, Unclassified, Confidential, Top Secret, NATO Secret, etc., a Yes response is required.)

If any of the above statements were answered with a "YES", provide a **detailed** description of the systems involved, the security controls employed, information shared, allowed accesses, number of foreign nationals, etc. and identify the Designated Approval Authority for that connection. Please be sure to sign and include the reference number on any and all attachments. Any questions may be directed to OAA IT&C, Director of Network Security Services – Pentagon, Connection Approval (CAP) Office at (703) 588-6597, DSN: 425-6597.

If this document and its attachments are classified after completion, please call the OAA IT&C CAP Office at DSN: 425-6597 to coordinate a secure transmittal. You may also return it by registered mail to the following address:

Director of Network Security Services - Pentagon
ATTN: SAAA-IT-NS
1777 North Kent Street (Suite 1500)
Arlington, VA 22209

CERTIFICATION: I certify that the information provided in this document and all attachments are accurate.

OR _____

Signature Block
Designated Approving Authority (DAA)

Signature Block
Information System Security Officer (ISSO)